**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?  
   It’s the assurance that data is accurate and reliable, and is available in a timely manner.
2. Biometrics
   1. Describe biometric security.  
      the use of physical human characteristics, including patterns or handwriting, to authenticate a user before granting them access to data.
   2. Why does it appeal to security managers?  
      it is nearly impossible to copy or steal a person’s biometric characteristics.
   3. List the common biometric devices.  
      Voice Recognition, fingerprint recognition, hand geometry, signature verification, facial recognition and iris recognition.
   4. What are the concerns of biometric technology?  
      intrusive o the technology, and cost.
3. Swipe cards
   1. Describe the nature of a swipe card.  
      business-card sized plastic card with a magnetic strip on one side and user details stamped or printed on the other.
   2. What is a limitation of the swipe card?  
      easily damaged by magnetic fields. If stolen, they offer little protection from a thief with a swipe-card reader that can capture the data on it.
4. Smart cards
5. Security tokens
6. Mobile phone secure code
   1. How does this level of authentication work?  
      Authentication occurs when a security code is sent to the account holder’s mobile phone to authenticate a transaction before it actually occurs. The account hold then need to log in and enter the code before the transaction is processed.

**Power protection**

Outline the characteristics of the following:

1. Surge protector  
   which protects electrical equipment against over voltage caused by a power surge.
2. Uninterruptible power supply, (UPS)  
   a UPS is a high-quality surge protector and battery built into the one device. Not only does it guard against a spike, but it will also help to protect data if there is an undercurrent or complete power failure.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?  
   Redundancy means no single part of the system is critical to its overall operation. If one part fails, the others – in this case, hard drives or mirrored machines – can take over its job and keep the system running until the part is replaced.
2. What is meant be a fault-tolerant server?  
   Will continue to work even when a piece of hardware has failed. This tolerance is achieved by having multiple components, such as dual hard drives, motherboards or power transformers, running in parallel.
3. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.  
      in this context redundancy means no single part of the system is critical to its overall operation. If one part fails, the other – in this case, hard drives of mirrored machines – can take over its job and keep the system running until the part is replaced.
   2. What is meant by RAID technology  
      a RAID is normally used on a computer network. In a RAID- protected system, fragments of data are spread over several hard drives, so that if one hard drive fails, the others can piece together the missing data and rebuild the file using error-checking codes.
4. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?  
      a mirrored computer is a more expensive option than using RAID because of the extra hardware involved. A RAID system requires a controller and the disk drives to be mounted in a rack, but fitted to a single server, whereas a duplicate server may cost many thousands of dollars more.

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?  
   - Magnetic media  
   -Optical drives  
   Solid-state drives.

Three categories of backup media:

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive  
   an affordable option is to back up files to a second internal hard disk. This is useful if you have many files. It is best to have a removable or external hard drive, otherwise in the case of a disaster, such as a fire or flood, the backup drive may be destroyed along with the original.
2. Magnetic tapes  
   Magnetic tapes are very popular form of media for backup files. They are relatively cheap, but very slow to save and restore files, as the tape must be read and accessed sequentially. If a file that is located near the end of a tape needs to be restored, the tape must be progressed past all the other material until the start point is reached.

**Optical media**

1. Compact disc  
   Compact discs are removable storage media and can hold up to 700MB of data and come either as CD-Read, which can only be used once to write data, or CD-RW, which allows you to write data to the disc a number of times.
2. DVD  
   With the amount of data being stored within home and organisational computers growing rapidly, the popularity of the DVD as a backup medium has grown.
3. Blu-ray  
   Blu-ray is a new optical disc format with a capacity of 50GB designed to replace the DVD format. The name ‘Blue-ray’ refers to the blue laser used to read the disc, which allows five times more storage than a DVD and allows high def. films to be filmed.

**Solid-state drives**

1. USB storage devices  
   USB keys or storage devices are a popular way of back up files. USB keys are small and often conveniently sold as a ‘key ring’ that toy can take anywhere. The benefit for the user is that there are no moving parts, as the memory is solid state, and therefore there is less chance of a breakdown.

**Online backups**

1. Why do organisations use this form of backup?  
   Faster communications links have made online backups more possible than ever before. Files can be backed up via the Internet to remote servers at data centres that have fault-tolerant servers, redundant power supplies, multiple Internet connections and uninterruptible power supplies.
2. Describe an enterprise storage system.  
   An enterprise storage system typically involves the interconnection via a storage area network (SAN), of RAID disks, tapes, CD/DVD-ROM, servers, Internet backup and other networked storage devices.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers  
   with most organisations now using networks, it is relatively easy to find out what people are sending to each other. Packet sniffers are diagnostic tools that monitor the contents of packets of data being sent across networks.
2. Desktop monitoring programs  
   Desktop monitoring programs work by intercepting ever single action performed on a computer. The monitoring program must be installed on the computer, but this can be done easily by an administrator either sitting at the computer itself, or remotely over the network.
3. Log files  
   Even without dedicated monitoring programs, computers already record most of what we do. Web servers record every URL accessed, who accessed it and how long they remained at that site. Similarly, our own web browsers store accessed webpages and images in a cache and keep a local file of our browsing history.
4. Closed-circuit television, (CCTV)  
   employers might be able to see what is happening at your computer, but they may also want to see what is happening in the workplace itself. This is particularly important in cases of workplace accidents or harassment.  
   Closed-circuit television (CCTV) consists of a series of video cameras linked to an internal TV system. Usually, they are watched by security guards who might have a monitor for each camera or have several cameras display on one screen.
5. Telephones  
   many spy films show secret agents listening in to or ‘tapping’ telephone conversations. Employers will often do the same. The reasons differ; depending on the type of work involved.
6. Audit trails  
   it is important that any access to an information system, and the transfer or modification of files is recorded so that if problems occur they can be traced back to the source. The combination of surveillance systems described above enable managers to trace transactions or any other form of activity in the system.

**Physical security devices:** List the options for physically securing your data